IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 4, Apr 2014, 53-62

EAACM: ENHANCED ACK AWARE CLUSTERING MECHANISM FOR ENERGY EFFICIENT AND SECURE ROUTING IN WIRELESS SENSOR NETWORKS

C. RAMKUMAR[1], H. R. PRADEEP KUMAR[2] & S. KRISHNAPRASANTH[3]

[1]Assistant Professor, Department of Electronics and Communication Engineering, SNS College of Engineering, Coimbatore, Tamil Nadu, India

[2,3]Under Graduate Scholar, Department of Electronics and Communication Engineering, Anna University, SNS College of Engineering, Coimbatore, Tamil Nadu, India

ABSTRACT

Wireless Sensor Network (WSN) is an emerging and very interesting technology applied to different applications. They are formed by little, self-deciding sensors that cooperate to form a large scale network with thousands of nodes covering a large area. Clustering the sensor nodes is an effective technique for achieve the energy efficiency of the network. Current clustering schemes utilize the two Passive Clustering schemes that create a hierarchical control structure for the clusters in the Wireless Sensor Networks; selecting the cluster heads with more residual energy, and rotating the cluster heads periodically to distribute the energy consumption among nodes in each cluster and prolong the network lifetime. The proposed system is Enhanced ACK Aware Clustering mechanism, called EAACM, to provide persistent routing path in Wireless Sensor Networks.

The EAACM introduces the Predicted Routing Path to assist in constructing the cluster head and gateway nodes. By determining the suitable Predicted Routing Path of the nodes in the cluster, the energy efficiency of the routing path will be increased, and by using the enhanced channel aware technique called ACKnowledgement Aware Detection for secure routing. An AAD uses the passive malicious node detection method, by measuring the time occurrence of ACK packets that are received by the source node. EAACM proposes the suitable efficient path for the ACK packet that increases the Energy-Efficiency and Secure-Routing by using ACK Aware Detection in Wireless Sensor Network. In AAD the ACK packet is sent after every node routing and also CH routing. If the ACK packet is delayed by the predefined time then the node is considered to be the malicious node and also that node will be avoided when routing. In case of the CH malicious node the next CH node will be elected according to the possible node from another possible route using the path provided by the PRP.

KEYWORDS: Wireless Sensor Network, Clustering Mechanism, Secure-Routing, Energy-Efficient Routing

INTRODUCTION

Recent advancement in wireless communications and electronics have led the development of low-power, low-cost, multifunctional small sensor nodes that are terribly tiny in size and have the shorter communication vary. These tiny sensor nodes, that incorporates sensing, computing, communicating the thought of sensor networks. A wireless sensor network describes a major improvement over typical sensor networks.

A sensor network is formed of an outsized range of sensor nodes that are densely deployed either within the

development or terribly almost it. The position of sensor nodes needn't be designed or planned. This enables random deployment in some applications. A number of the appliance areas are military and health, etc. In wireless sensor networks (WSNs), security and energy consumption are thought-about as durable technical challenges as sensors typically suffer from complexness and energy constraints. In typical WSNs, sensor nodes should report the sensing or monitoring information to a central node, known as the sink, once receiving query messages sent by the sink [1] [2]. As a result of sensor nodes are terribly small and internal battery powered devices, charging the batteries for sensor nodes is usually difficult. Operations, like sensing, communication, and computation and data transmission is that the major source of energy consumption. From military to civilian applications, binary distributed detection issues in wireless sensor networks (WSNs) are enclosed in an exceedingly wide selection of area like military, police investigation, inventory management, and lots of others. Early warning system like intrusion detection [1], [2] and disaster alert, network management within the self-organized network, and spectrum sensing within the cognitive radio are the notable ones that the binary distributed detection is applied to forestall a possible conflict or crisis.

However, the transmittal nature of wireless communications makes the distributed detection at risk of intrusion or eavesdropping [2] [10] [12]. Moreover, in apply, sensors for the distributed detection in WSNs are usually incapable of using typical crypto-graphical techniques as a result of sensible constraints of sensors like restricted energy resources, computing power, etc. Thus, for sure the attackers would have an opportunity to disrupt or management the whole network simply by monitoring sensors observations. Thus, it is a heavy challenge to implement an energy efficient and secure communication theme for coverage sensory data to attain a high delivery ratio and prolong the network life with secure communication.

BACKGROUND OF CLUSTERING

Heed- Clustering Approach

In Hybrid, Energy-Efficient Approach, HEED [4] protocol that periodically selects cluster heads according to a hybrid of their Primary and Secondary node parameters. Where the first parameter defines the Residual-Energy and the second parameter describes the Node Proximity to its neighbour nodes or the Node-Density [3]. A Residual-Energy as a first parameter is directly known since the energy consumed per bit for sensing, computing and communicating is typically known. The secondary parameter consists of intra-cluster communication cost. Here the cost can be a function of neighbour proximity or cluster density. It uses the primary parameter to probabilistically select an initial set of cluster heads, and the secondary parameter to break ties. A tie in this reference means that a node falls within the range of more than one cluster head, including the situation when two tentative cluster heads fall within the same range. The main aim of the EAACM is to obtain the secure routing in the energy efficient manner. In EAACM the cluster head and gateway nodes are chosen by the energy efficient passive clustering technique by measuring the parameter PRP (Predicted Routing Path) and the secure transmission of packets is ensured by utilizing one of the PRP as an ACK path for receiving the ACK packet from destination to source.

Unequal Clustering Scheme

In Unequal Cluster based Routing (UCR), [5] the hot spot problem due to the traffic relay in the cluster head which is in near to the base station is appreciably avoided in the UCR.

Traffic relay is mainly due to the multi-hop sensor network. In multi-hop sensor networks the cluster head of the

cluster which is in closer to the base station is congested with the data packets due to the all clusters transmit the sensing information to the base station through that cluster. So the energy consumption of that cluster is reasonably high because of intra-cluster communication and traffic relay problem. So, to avoid the much more energy consumption in that particular cluster, the cluster size and density is made variable with the function of distance from the base station. The cluster which is in very near to the base station is made very small to avoid more number of intra-cluster communications, so the energy efficient is increased. But it makes the sensor network with unequal density and this is the main disadvantage of the UCR. In EAACM the channel formed between the two nodes are utilized in the form of many clusters with the same density to choose the suitable cluster head and gateway nodes by measuring the parameter PRP of each node.

DISTRIBUTED ENERGY-EFFICIENT CLUSTERING ALGORITHM

The clustering algorithmic rule could be a quite key technique used to cut back energy consumption. It will increase the measurability and lifetime of the network. Energy-efficient clustering protocols ought to be designed for the characteristic of heterogeneous wireless sensor networks. In DEEC, the cluster-heads are elected by a likelihood supported the quantitative relation between residual energy of every node and also the average energy of the network. The epochs of cluster head for nodes are completely different consistent with their initial and residual energy. Nodes with the high initial and residual energy can have a lot of probabilities to be the cluster-heads than the nodes with low energy. Finally, the simulation results show that DEEC [6] achieves longer lifetime and more effective messages than current vital clustering protocols in heterogeneous environments. However, within the EAACM the cluster head is chosen within the turned manner with calculated parameter referred to as PRP. By measuring the PRP every node in each cluster the acceptable CH and gateway node may be chosen to extend the network lifespan and therefore the energy efficient is increased relatively.

ENERGY EFFICIENT CLUSTERING SOLUTION FOR WIRELESS SENSOR NETWORK

Hot spots [7] during a wireless sensor network emerge as locations underneath in a traffic load. Nodes in such areas quickly consume energy resources, resulting in disruption in network services. This downside is common for data assortment situations during which Cluster Heads (CH) have a significant burden of gathering and relaying data. The relay load on CHs particularly intensifies because the distance to the sink decreases. To balance the traffic load and the energy consumption within the network, the CH role ought to be turned among all nodes and the cluster sizes ought to be fastidiously determined at completely different parts of the network.

This paper proposes a distributed clustering algorithmic rule, Energy-efficient clustering (EC) that determines appropriate cluster sizes counting on the hop distance to the info sink, whereas achieving approximate levelling of node lifetimes and reduced energy consumption levels. We tend to in addition propose an easy energy-efficient multi-hop data collection protocol to gauge the effectiveness of EC and calculate the end-to-end energy consumption of this protocol; however EC is appropriate for any data collection protocol that focuses on energy conservation. Performance results demonstrate that EC extends network period of time and achieves energy levelling more effectively than two well-known clustering algorithms, HEED [4] and UCR [5]. However within the EAACM the cluster head is chosen within the cluster with calculated parameter referred to as PRP. By activity the PRP of every node in each cluster the acceptable Cluster Head and gateway node may be chosen to extend the network period of time and also the energy efficient is inflated relatively.

OVERVIEW OF AN EAACM

The proposed method consists of three main blocks; they are,

- Predicted Routing Path and Link Failure Maintenance.
- Clustering Mechanism for Energy Efficient routing.
- ACK Routing for Malicious Node Detection.

PREDICTED ROUTING PATH AND LINK FAILURE MAINTENANCE

Many routing protocols have been developed for mobile ad-hoc wireless network.

When a host or node wants to send a message to destination-node and does not have a valid route to that destination-node, it initiates a route discovery process in order to find out the destination node. Then, it broadcasts a route request (RREQ) packet to its neighbours, which forwards the request to its neighbours until it reaches the desired destination-node or reaches intermediate node which has information about the route to the destination-node [8]. During the route discovery processing, each intermediate node recodes its own sequence number (called broadcast ID). This broadcast ID is incremented for every RREQ that the node initiates, and also records the nodes IP address (source and destination IP addresses).

Intermediate nodes can reply the RREQ, in case they have a route to the desired destination-node, only if the destination sequence number is greater than or equal to that contained in the RREQ [9].

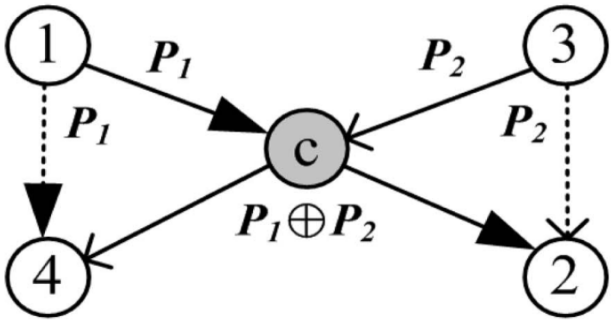

Figure 1: Coding Node and Route Discovery

For this purpose, the re-routing protocol is implemented which works as follows:

This new mechanism uses the link state prediction method for predicating an active link. In addition, it will use one hop neighbours to collect their signal status. Consider two nodes X and Y and if there is any link failure between nodes X and Y, then the mechanism is as follows: After the link state predication algorithm informs that the link between X and Y will be broken soon, node X takes an action to sort out the matter, instead of sending warning message back to the sender as in AODV traditional mechanism node X circulates a local route request to neighbours except the node that node X is receiving from to check signal status and whether there is a route to the destination. If current node (in this case, node “X”) could not receive a positive response from its neighbours (because no one has a route to the desired destination or maybe they do not have a stronger signal than the current connection), the current node (X) will send a notification to previous node (one hop to upstream) indicating the link will be broken soon.

CLUSTERING MECHANISM FOR ENERGY EFFICIENT ROUTING

In EAACMM the novel PRP measurement is the first and foremost metric used for the cluster head selection. The nodes in the PRP will only be selected for the Cluster Head and Gateway node to minimize the inter cluster communication cost. Among the set of sensor nodes the nodes in the PRP will act as a cluster head with certain cluster limit, like this many clusters are formed with the suitable cluster heads and gateway nodes.

ACK AWARE DETECTION FOR MALICIOUS NODE DETECTION (SECURE ROUTING)

In EAACM the malicious node is detected in the each cluster by measuring the time elapsed between the receiving packets and receiving ACK of each node while communicating [Packet Forwarding]. Because the channel strength is equal to the pre measured value as the bandwidth of the channel is constant over the entire communication MAC [1], [2]. Any changes in the channel strength affect the receiving of ACK packet, that the possible of malicious node in the Cluster and these nodes can be eliminated from further consideration of routing.

In EAACM, AAD method is used to detect the malicious node within the cluster and also between the Cluster Head (CH) nodes in the case of CH malicious node. In AAD the ACK packet is sent after every node routing and also CH routing. If the ACK packet is delayed by the predefined time then the node is considered to be the malicious node and also that node will be avoided when routing. In case of the CH malicious node the next CH node will be elected according to the possible node from another possible route using the PRP.

This process will not exceed normal run time due to the ACK packet delivery because, we have already ACK path in PRP scheme. This path can be used for the ACK packet delivery. So energy efficient and secure routing is achieved without more usage of resources.

The novel EAACM technique consists of these three factors to obtain the Energy-Efficient and Secure Routing.

- **Predicted Path Routing:** This mechanism is used to find the shortest path with in all the nodes in the sensor network.
- **Clustering Mechanism:** This block consists of the ‘Clustering Process’ which is used to elect the suitable sensor node into cluster head and gateway nodes.
- **Enhanced ACK Aware Clustering Mechanism:** This block is used to detect the malicious node among each cluster.

Overview of the project is to establish the Energy-Efficient Routing and the Secure-Routing among the network.

PROTOCOL OF EAACM

Local Route Request (LRREQ)

LRREQ comes up with a very useful mechanism on link failure route maintenance. LRREQ mechanism is used when the link state prediction model notifies that the link between two intermediate nodes on an active link will be broken soon.

This means that, when the A-B link is going be collapsed soon, node A takes an action to sort out the matter, instead of sending warning message back to the sender. In this respect, node A circulates a Local Route Request (LRREQ)

among its neighbours, except the node that node A is receiving from (it does not circulate to upstream node), to find out if there is a node that has a stronger signal than downstream node (in this case, the downstream node is "B") and, at the same time, has a route to the destination. In addition, a LRREQ with beacon mechanism will use one hop neighbours to collect their signal status. LRREQ mechanism uses one hop range.

The new mechanism, LRREQ, uses the link state prediction method, as well, for predicating an active link. In addition, a LRREQ with beacon mechanism will use one hop neighbours to collect their signal status.

LRREQ mechanism uses one hop range. Suppose consider the two nodes A and B and if the link between these two nodes get lost then the mechanism is as follows:

After the link state predication algorithm informs that the link between A and B will be broken soon node A circulates a local route request to neighbours to check signal status and whether there is a route to the destination. If current node (in this case, node "A") could not receive a positive response from its neighbours (because no one has a route to the desired destination or maybe they do not have a stronger signal than the current connection), the current node (A) will send a notification to previous node (one hop to upstream) indicating the link will be broken soon. Thus, when this node (the upstream node) receives such notification from the next hop (downstream), it circulates a Local Route Request into its neighbours except the upstream one and so on. The upstream notification continues until a new route to the desired destination is found. The proposed mechanism is expected to improve the network performance significantly, reduces network overhead, decreases the packet loss, reduce end-to-end packet delays, increase the throughput, utilize the network resources efficiently and improve packet delivery ratio.

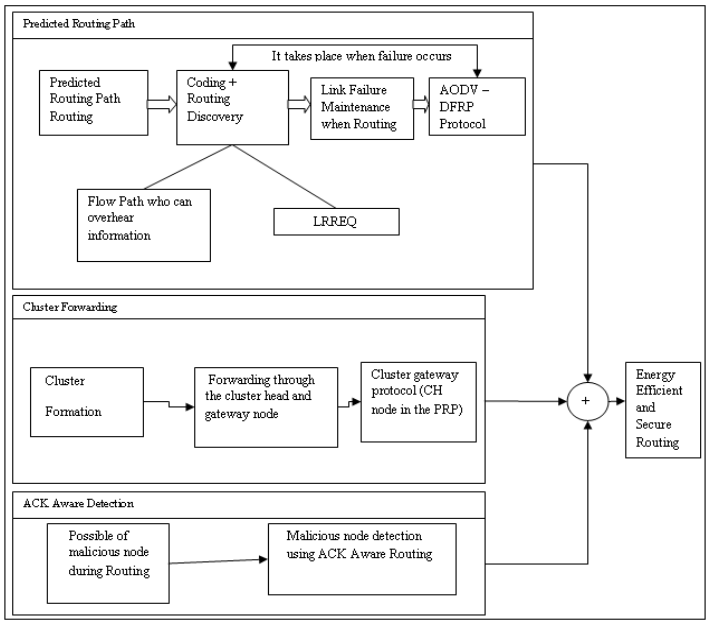

Figure 2: Overview of an EAACM

RESULTS AND DISCUSSIONS

In the EAACM mechanism there are different kind of routing path (Shortest path) be assigned which will handle the link failure cases in the network. There is "Link Handling" routing path of the network is assigned to make proper path for routing in the Link failure condition.

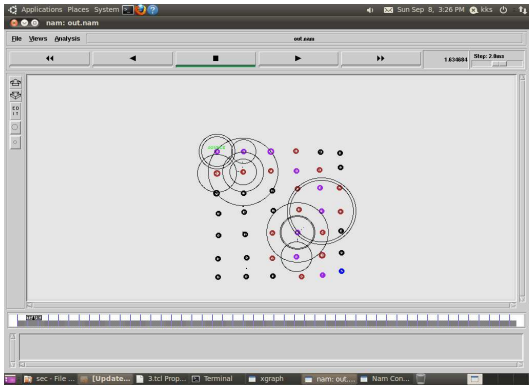

Figure 3: Link Failure Maintenance

ROUTING WITH CLUSTER HEAD FORWARDING

With the normal flow of packets in the network, the link failure is introduced in the network. The link failure occurrence in the network is differentiated. The packet delay is measured before and after the link failure occurrence in the network. Also the throughput of the network when the link failure occurs and after the link failure recovery has also been measured.

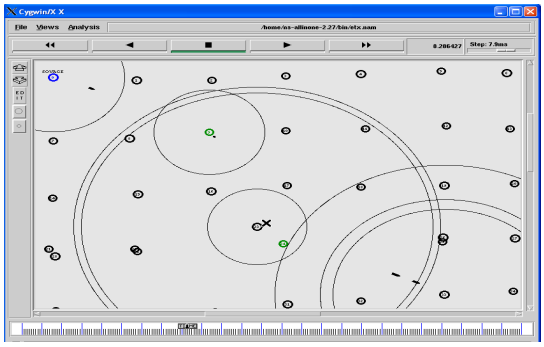

Figure 4: Cluster Head Forwarding

ENERGY CONSUMPTION

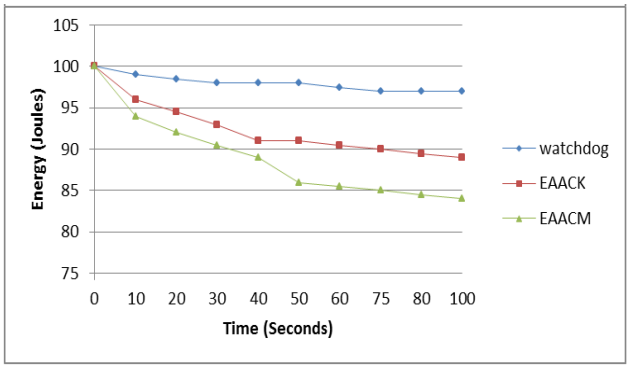

Figure 5: Energy Graph

Amount of energy consumed in an EAACM is very less when compared to other counter parts such as Watch dog and EAACK.

From the graph, proposed EAACM has the high Energy-Efficient routing through the network.

PACKET DELIVERY RATIO

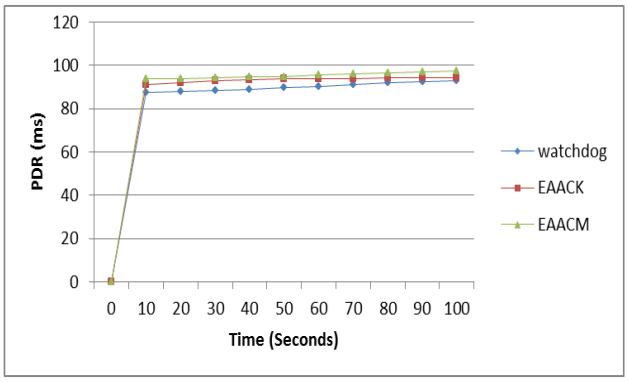

Figure 6: Packet Delivery Ratio

The ratio of the number of delivered data packet to the total data packets arriving to the destination is high in EAACM.

PACKETS RECEIVED

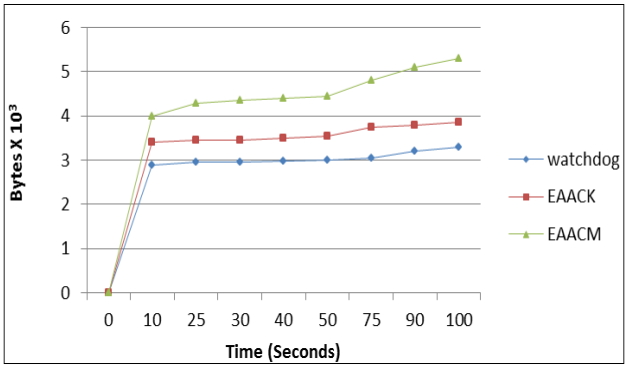

Figure 7: Packets Received

Number of packets received in the EAACM is relatively high than the EAACK and watchdog

OVERHEAD

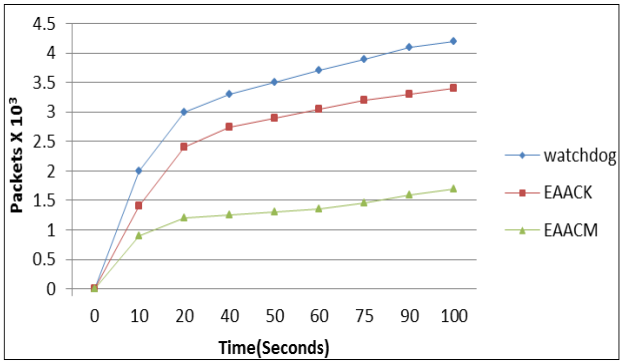

Figure 8: Overhead of EAACM

Processing time (Overhead) required for the network with EAACM is very low when compared to other schemes such as EAACK and Watchdog.

CONCLUSIONS

Thus the novel EAACM technique comparatively provides highly Energy-Efficient routing among other current schemes of routing. This routing scheme also helps to avoid the Link-Failure and the Packet-Loss while routing the packet through the nodes, because the data packets are sent through the PRP of the network.

The ACK Aware Detection (AAD) method in the sensor networks provides highly secured routing which helps the sensor networks from the passive eavesdropping.

FUTURE WORK

Future work of EAACM includes that; this research can also be influenced in to the Mobile Ad-hoc Network (MANET) for data aggregation into and from the server.

ACKNOWLEDGEMENTS

We express our sincere thanks to all the faculty members of Electronics and Communication department in SNS College of Engineering, especially our Head of the Department and Our Project guide.

REFERENCES

1. Akyildiz, F., Su, W., Sankara subramaniam, Y and Cayirci, E 1992 “A survey on sensor networks,” IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114.
2. Ameer Ahmed Abbasi, Mohamed Younis 2002 “A survey on clustering algorithms for wireless sensor networks”.
3. Younis, O and Fahmy, S 2004 “HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks,” IEEE Trans. Mobile Comput.
4. Chen, G., Li, C., Ye, M and Wu, J. 2009 “An unequal cluster-based routing protocol in wireless sensor networks,” Wireless Networks vol. 15, no. 2, pp. 193–207.
5. Ossama Younis and Sonia Fahmy Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach.
6. Wei, D., Jin, Y., Vural, S., Moessner, K and Tafazolli, R 2011 “An energy efficient clustering solution for wireless sensor networks,” IEEE Trans. Wireless Commun., vol. 10, no. 11, pp. 3973–3983.
7. Christina, F., Dina, K., Athina, M., Muriel, M. and Hariharan, R. 2007 ‘Wireless Network Coding: Opportunities & Challenges’, Military Communications Conference, MILCOM 2007, IEEE, pp. 1-8.
8. Douglas, S.J.D.C., Daniel, A., John, B and Robert, M. 2003 “A High-throughput Path Metric for Multi-hop Wireless Routing”, In ACM MobiCom ’03, San Diego, California, pp. 134-146.
9. Dorothy E. Denning "An Intrusion-detection Model” 1987 IEEE Transaction on Software Engineering, **13**, No. 7, pp 222-232, Feb 1987.
10. B. Sun, K. Wu, and U. Pooch. “Zone-based Intrusion Detection for Mobile Ad hoc Networks”. Int. Journal of Ad Hoc and Sensor Wireless Networks, **2(3)**, 2003.

11. Tiranuch Anantvalee and Jie Wu "A Survey on Intrusion Detection in Mobile Ad Hoc Networks" 2004.
12. "An introduction to Network Simulator NS2" by TeerawatIssariyakul, Ekram Hossain. ISBN: 978-0-38-7-71759-3, DOI: 10.1007/978-0-387-71760-9, e-ISBN: 778-0-387-71760.
13. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.
14. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.
15. T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.
16. Elhadi M Shakshuki, Nan Kang and Tarek Sheltami, "EAACK: A Secure Intrusion Detection System for MANET" IEEE Transactions on Industrial Electronics, Vol. 60, No.3, MARCH 2013.